Title	Security Web Pen. Testing
Long Title	Security Web Penetration Testing
Credits	**5**
NFQ Level	Expert
Module Author	Anlia Mjeda

Module Description:

This module focuses on web penetration testing. The module explores various web pen-testing techniques and industry-standard tools. This module was developed under the Cyber Skills HCI Pillar 3 Project. Please refer to the consortium agreement for ownership.

Learning Outcomes

On successful completion of this module the learner will be able to:

LO1	Critically assess the steps involved in understanding, planning, and formalizing the scope of a penetration test.
LO2	Critically assess a web application's security posture, its vulnerabilities and the core vulnerabilities of its underlying network/s.
LO3	Develop effective exploitation techniques.
LO4	Create effective penetration testing reporting according to the industry guidelines and the state of the art.
LO5	Investigate the ethical aspects of ethical hacking.

Indicative Content

Setting the Scope

The activities that should happen before penetration testing takes place. Understanding, agreeing and formalizing the scope of the penetration test. Identifying the milestones when penetration testing is most beneficial.

Information Gathering

Traditional and modern security attacks techniques to protect modern applications. Common vulnerabilities such as the OWASP Top 10 and their exploits. Assessing websites and finding vulnerabilities. Spidering, scanning, fingerprinting web servers and OS, network mapping. Using tools such as OWASPZap, Burp Suite, DirBuster, Nikto, Metasploit, Nmap.

Exploitation

The ethics of exploitation (ethical hacking), the mindset and techniques of non-destructive penetration testing. Efficient communication with the technical and non-technical stakeholders. Manipulating URL parameters, cross-site scripting, SQL injections, hijacking sessions, etc

Reporting

Writing an informative report. Tailoring reporting templates to the need of the organization. Helping the client understand the findings of the penetration test.

Course Work

Assessment Type	*Assessment Description*	*Outcome Addressed*	*% of Total*	*Assessment Date*
Critique	The student may be expected to present a portfolio of penetration testing artefacts and a report on the current state of the art of Web Penetration Testing and its ethical aspects.	1,2,5	40.0	Week 7
Project	A project that follows the full cycle of a penetration test, including setting the scope, information gathering, exploitation, reporting and a critical analysis of the ethical aspects.	1,2,3,4,5	60.0	Sem End

No End of Module Formal Examination

Assessment Breakdown	**%**
Coursework	100

Re-Assessment Requirement

Coursework

This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.

Workload – Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lectures covering the theoretical concepts underpinning the learning outcomes	2.0	Every Week	2.0
Lab	Lab to support the learning outcomes.	2.0	Every Week	2.0
Independent & Directed Learning (Non-contact)	Independent learning by the student.	3.0	Every Week	3.0
		Total Hours		7
		Total Weekly Learner Workload		7
		Total Weekly Contact Hours		4

Workload – Part Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Leaner Workload*

Lecture	Lectures covering the theoretical concepts underpinning the learning outcomes.	2.0	Every Week	2.0
Lab	Lab to support the learning outcomes.	2.0	Every Week	2.0
Independent & Directed Learning (Non-contact)	Independent learning by the student.	3.0	Every Week	3.0
		Total Hours		7
		Total Weekly Learner Workload		7
		Total Weekly Contact Hours		4

Recommended Book Resources

- **OWASP, Elie Saad, Rick Mitchell, et al. 2020, *Web Security Testing Guide*, OWASP https://owasp.org/www-project-web-security-testing-guide/stable/**

Supplementary Book Resources

- **Dafydd Stuttard, Marcus Pinto 2011, The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Second Edition, John Wiley & Sons [ISBN: 978-1-118-026]**
- **Andrew Hoffman 2020, Web Application Security, O'Reilly [ISBN: 978-1-492-087]**
- **Peter Kim 2018, The Hacker Playbook 3: Practical Guide To Penetration Testing, Secure Planet [ISBN: 9781980901754]**
- **Laura Bell, Michael Brunton-Spall, Rich Smith, Jim Bird 2017, Agile Application Security: Enabling Security in a Continuous Delivery Pipeline, O'Reilly [ISBN: 978-149193884]**